Software Considerations in Highly Reliable Systems Development

Jasjit Heckathorn

Draper Laboratory

Software Considerations in Highly Reliable Systems Development

- Software issues in Systems Development and Maintenance
- Software Systems Engineering
- Software Systems Engineering Practice at Draper

Software issues in Systems Development and Maintenance

- Systems are becoming larger, software intensive, and complex
  - Software is managing the increasing complexity of systems
  - Software provides the cohesiveness and control of data
  - Software provides the flexibility to work around/correct hardware or other problems that are found late in the development cycle
- Software cost is becoming the biggest driver of life cycle system cost since maintenance cost is mostly due to software changes required to
  - Respond to changing system requirements
  - Add functionality
  - Correct software or hardware problems
  - Upgrade obsolete hardware or COTS configuration
- Major systems failures are attributable to software failures
  - Ariane 5
  - Mars Pathfinder

Software Systems Engineering

- Application of appropriate software engineering technologies and processes to transform an operational need into a high quality and cost effective product
  - Technical considerations
  - Management considerations
- Technical considerations
  - System requirements and design
    - » Partitioning and allocation to software
    - » Hardware software trade-offs
  - Software requirements analysis
    - » Modeling
    - » Requirements specification and verification
  - Software design
    - » Use of design principles to facilitate maintainability and supportability
    - » Design documents

Software Systems Engineering

- Technical considerations (cont)
  - Code and unit test
  - Software integration and test
    - » Test Documentation
    - » Hardware simulations
    - » Software fault seeding
    - » Operational Scenarios
    - » Stress tests
  - Software/ hardware integration and test
    - » Interface tests
    - » Timing tests
    - » Hardware in the loop tests
  - System test

Software Systems Engineering

- Management Considerations
  - Requirements management
    - » Traceability
    - » Impact of change
  - Software planning
    - » Size, cost and schedule estimation
    - » Development approach (incremental, evolutionarily, spiral, prototype)
    - » Risk assessment
    - » Reuse, COTS considerations
    - » Products and Reviews
    - » Development environment
      - Methodologies and tools
    - » Test process and test environment

Software Systems Engineering

- **Management Considerations(cont)**
  - **Software tracking and oversight**
    - » **Status reviews and design reviews**
    - » **Metrics**
  - **Software configuration management**
    - » **Baseline management**
    - » **Software build management**
  - **Software quality assurance**
  - **Communication and coordination**

Software Systems Engineering Practice at Draper

- **Draper provides innovative technical solutions associated with complex dynamic systems that must be highly reliable**
  - **Technical, reliability and safety considerations are and have always been of vital importance**
- **Recently management considerations have gained attention through the software process improvement initiative**
  - **Achieved SEI Maturity Level 3 in June 97**
  - **Standard process for the entire software development cycle exists and software engineering staff is trained**
  - **Projects use the Tailoring Guidelines to develop a software project plan, follow the plan and are monitored and audited against it**
  - **Projects Asset database contains methods, procedures, templates, tools, samples and Lessons Learned on projects**
  - **Metrics database is being populated for use in estimation**
  - **New technologies and tools are evaluated and inserted in projects**

Software Systems Engineering Practice at Draper

- **Legacy Systems Development Experience**
  - **A10 CDU version 1 1991- 1995**
    - » **Purpose - Integrate GPS into aircraft, and loosely couple with Inertial Nav System**
      - **New CDU hardware and software to couple the GPS and INS and control Improved Data Modem (IDM) communications**
    - » **Technologies**
      - **Object oriented design, Ada and assembly mix**
        - **Cadre Teamwork**
        - **Host VAX, Target Motorola 68020**
        - **XDAda (enhanced for for real-time tasking requirements)**
        - **In-circuit-emulator, Hardware-in-the-loop, Hot Bench**
    - » **DOD-STD-2167A process**
      - **Software Development Plan**
      - **Requirements management (home grown tool)**
      - **Configuration management (VaxCMS)**
      - **Tracking and Oversight (PS5, status meetings, software problem reports, user meetings, customer reviews)**
      - **Peer reviews**
      - **SQA and IV&V**

Software Systems Engineering Practice at Draper

- **Legacy Systems Development Experience**
  - **A10 CDU version 2 1996- 1998**
    - » **Purpose - Replace existing GPS and INS with Honeywell supplied Embedded GPS/INS (EGI)**
    - » **Technologies**
      - **Object oriented design, Ada and assembly mix**
        - **Host VAX, Target Motorola 68030**
        - **XDAda (enhanced for real-time tasking requirements)**
        - **In-circuit-emulation, Hardware-in-the-loop, CAST simulator and INS simulator, Hot Bench**
        - **COTS integration**
    - » **DOD-STD-2167A process enhanced with Standard Draper process**
      - **Software Development Plan**
      - **Requirements management (home grown tool)**
      - **Configuration management (Vax CMS, added scripts, automated build process)**
      - **Tracking and Oversight (MS Project, home grown metrics and problem tracking tool, user meetings, customer reviews)**
      - **SQA and IV&V**
      - **Peer reviews**

Software Systems Engineering Practice at Draper

- **Legacy Systems Development Experience**
  - **GPS Ground Stations Replacement 1993-1995**
    - **Purpose - Develop system design to replace obsolete computer hardware and software in GPS Ground Antenna and Monitor Stations**
    - **Unique technical approach for analyzing requirements for legacy systems using existing documentation and discussions with users and maintainers of software**
      - **System requirements**
        - **Multiple views of the system (Behavioral, structural, data)**
        - **System Segment Specification (DOD-STD-2167A)**
      - **System Design**
        - **Reliability, maintainability, extensibility, supportability considerations**
        - **Open System Architecture, compliant with Industry standards**
        - **System Design Document (DOD-STD-2167A)**
      - **Software Requirements**
        - **Object Oriented Analysis (Rumbaugh)**
        - **Software Requirements Specification (DOD-STD-2167A)**
    - **Process**
      - **Project plan**
      - **Methodology and tool assessment followed by team training**
      - **Requirements traceability (RTM)**

Software Systems Engineering Practice at Draper

- **New Systems Development Experience**
  - **Advanced Seal Delivery System (ASDS) 1994-1997**
    - **Purpose - Provide guidance, navigation and control for manned submersibles and develop Integrated Control and Display (ICAD) processing**
      - Graphical Users Interface (GUI)
      - Performance Monitoring Fault Localization (PMFL)
    - **Software Architecture and Top Level Design Reused from fielded Deep Submergence Rescue Vehicle (DSRV)**
      - Host Sun, Target 68040 , C programming language
      - Reverse Engineer DSRV Software (Hindsight 20/20)
      - COTS Operating System (VxWorks)
      - Hardware in the loop
    - **Mil-STD-498 process enhanced with Standard Draper Process**
      - Detailed software development plan
      - Requirements Management (home grown tool)
      - Configuration Management (Continus)
      - Tracking and Oversight (PS5, MS Project, home grown metrics and problem tracking tool, user meetings, customer reviews, unit test coverage, risk management)
      - SQA and IV&V
      - Peer reviews

Software Systems Engineering Practice at Draper

- **New Systems Development Experience**
  - **Simulation Based Test and Evaluation Capability(SiBaTEC)1995-1998**
    - » **Purpose - Develop a user friendly real-time simulation facility that allows guidance systems developers to formulate and test performance and technology hypotheses**
      - **Graphical User Interface (GUI)**
      - **3D animations**
    - » **State-of-the-art technologies, development environment and design tools**
      - **Object oriented analysis and design, C++**
        - **Multiple platforms (Solaris, IRIX, VxWorks, NT/95)**
        - **Rose, Purify, Quantify**
    - » **Standard Draper process facilitated by tools, with incremental development**
      - **Software development plan**
      - **Requirements Management (DOORS)**
      - **Configuration Management (Clearcase)**
      - **Tracking and oversight (MS Project and home grown metrics tool, collocated team, user meetings, regular status meetings with team and management, and customer/user reviews, risk list, process audits)**
      - **Peer reviews**

Software Systems Engineering Practice at Draper

- **Summary**
  - **Technical considerations and management considerations work hand in hand to produce a highly reliable, safe and cost effective system**
  - **Use new technologies and tools, but assess risks and have a mitigation plan**
    - **» COTS can work both ways**
  - **Design reviews, peer reviews are very helpful in early error detection**
    - **» Involve users, customers and other groups that have interfaces**
  - **A process appropriate for the end use of the system can provide visibility, mitigate risk and enhance quality**
    - **» Planning, requirements management, configuration management, tracking and oversight, and risk management can help control cost**
  - **Communication and coordination among the various developers can prevent a lot of interface problems and save time during system integration**